Remarks

Claims 1-19 are pending. Claims 1-19 are rejected.

In response to Examiner's restriction requirement, Applicants' elect claims 1-19.

Applicants' Attorney notes Examiner's provisional obviousness-type double patenting rejection over Application No. 10/119,204.

Claims 1-6, 8, 11-14 and 16-17 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Davis et al. (hereinafter Davis) U.S. Patent 6,088,450 in view of Zadok et al., Cryptfs: A Stackable Vnode (hereinafter Zadok) and in view of Teppler U.S. Patent 6,792,536. Claims 7 and 15 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Davis in view of Zadok and in view of Teppler and further in view of Tagawa et al. (hereinafter Tagawa) U.S. Patent 7,096,504. Claims 9-10 and 18-19 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Davis in view of Zadok and in view of Teppler and further in view of Masuda et al. (hereinafter Masuda) U.S. Patent 6,714,649.

With regard to claims 1 and 12, one of ordinary skill would not have been motivated to combine Davis and Teppler. Davis teaches away from the use of a cryptographic subsystem because encrypting/decrypting data plays no role in achieving the goal of "mitigat[ing] the likelihood of unauthorized use of an electronic device through periodic challenge/response messages." Col. 1, ll.26-28 (emphasis added). Rather, Davis denies access to the node when its security device is outside the range:

> [t]he first successful Challenge/Response message exchange between the security device and the token places the node in an operational state allowing the authorized user access to the contents and/or networked resources of the node. Later Challenge/Response message exchanges are set to occur periodically to check whether the authorized user possessing the

> token has left the node unattended thereby causing the node to be placed in a non-operational state.
>
> Abstract
>
> the user is denied access to the node by any conventional manner such as by displaying a screen-obscuring image, refusing further input from the keyboard, mouse, etc., suspending further I/O to and from the node or suspending any network connections for a computer representing the node.
>
> Col. 6, ll. 37-42.

Furthermore, Teppler attempts to solve the problem of "proving . . . dates and times associated with access, creation, modification, receipt, or transmission of . . . [a] digital file." Col. 1, ll. 33-36. Davis and Teppler address different problems with different mechanisms.

With regard to claims 2, 13 and 14, Davis fails to teach, disclose, or suggest wherein the requests include cryptographic requests for cryptographic information and wherein the server supplies the cryptographic information in response to the cryptographic requests and wherein the cryptographic subsystem utilizes the cryptographic information to either encrypt or decrypt the data. Davis states that

> the node, namely the security device 210, may generate a random number ("RN") 500 and transmit RN 500 in a non-encrypted format as a Challenge message to the token 120. Upon receiving the Challenge message, the token 120 encrypts RN 500 with its private key "PRT", forming a Response message 505 and returns the Response message 505 back to the security device 210. Thereafter, the security device 210 decrypts the Response message 505 with a public key of the token "PUT" and checks to verify that the random number received ("RN_{rec}") 510 is equivalent to RN 500.
>
> Another example is that the security device 210 may produce a Challenge message 525 by generating a random number "RN" 520 and encrypting RN 520 with the token's public key "PUT" stored within the security device 210. Thereafter, the Challenge message 525 is transmitted to the token 120. Upon receiving the Challenge message 525, the token 120 decrypts the Challenge message 525 with its private key "PRT" to retrieve the random number "RN_{trnt}" 530.

> Thereafter, RN_{trnu} 530 is transmitted back to the security device 210 and compared with RN 520 previously transmitted to determine if they are equivalent. If so, the user is provided access to the data stored within the node and if not, the user is prevented such access.
>
> Col. 6, l. 55 - col. 7, l. 11.

In the first example, the security device 210 transmits a random number in a non-encrypted format to the token 120, col. 6, ll. 55-58. In the second example, the token 120 transmits a random number in a non-encrypted format to the security device 210. Morever, Davis does not use its random number to encrypt or decrypt data. Rather, it merely uses it in deciding whether to provide access.

The dependent claims are patentable at least because they depend from one of the independent claims.

Applicants' Attorney has made a genuine effort to respond to Examiner's rejections in advancing the prosecution of this case. Applicants' Attorney believe all formal and substantive requirements for patentability have been met and that this case is in condition for allowance, which action is respectfully requested.

If Examiner believes that a phone conversation will expedite prosecution of this Application, Examiner is strongly encouraged to contact me at (248) 358-4400.

Please charge any fees or credit any overpayments as a result of the filing of this paper to our Deposit Account No. 02-3978.

Respectfully submitted,

BRIAN D. NOBLE, et al.

By 

Benjamin C. Stasa
Reg. No. 55,644
Attorney for Applicants

Date: January 17, 2007

BROOKS KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075-1238
Phone: 248-358-4400
Fax: 248-358-3351